

ON A UNIFORMLY DISTRIBUTED PHENOMENON IN MATRIX GROUPS

SU HU AND YAN LI

ABSTRACT. We show that a classical uniformly distributed phenomenon for an element and its inverse in $(\mathbb{Z}/n\mathbb{Z})^*$ also exists in $\mathrm{GL}_n(\mathbb{F}_p)$ and $\mathrm{SL}_n(\mathbb{F}_p)$. A $\mathrm{GL}_n(\mathbb{F}_p)$ analog of the uniform distribution on modular hyperbolas has also been considered.

1. INTRODUCTION

The distance between an element $x \in (\mathbb{Z}/n\mathbb{Z})^*$ and its inverse $x^{-1} \pmod{n}$ has been studied by many authors [1, 4, 6, 9, 12, 13]. Shparlinski [10] gave a survey of a variety of recent results about the distribution and some geometric properties of points (x, y) on modular hyperbolas $xy \equiv a \pmod{n}$.

Denote by $\{x\}$ the fractional part of a real number x . Let

$$f_n : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow [0, 1] \times [0, 1]$$

$$x \mapsto \left(\left\{ \frac{x}{n} \right\}, \left\{ \frac{x^{-1}}{n} \right\} \right).$$

By using the Erdős-Turán-Koksma inequality and the Weil-Esternmann inequality for Kloosterman sum, Beck and Khan [1] gave an elegant proof for the following classical result.

Theorem 1.1. *Let $R \subset [0, 1]^2$ be a measurable set having the following property that for every $\epsilon > 0$, there exist two finite collections of non-overlapping rectangles R_1, \dots, R_k and R^1, \dots, R^l such that $\cup_{i=1}^k R_i \subseteq R \subseteq \cup_{j=1}^l R^j$, $\mathrm{area}(R \setminus \cup_{i=1}^k R_i) < \epsilon$ and $\mathrm{area}(\cup_{j=1}^l R^j \setminus R) < \epsilon$. Then*

$$\lim_{n \rightarrow \infty} \frac{\mathrm{cardinality}(\mathrm{Image}(f_n) \cap R)}{\varphi(n)} = \mathrm{area}(R).$$

Remark 1.2. Notice that, our statement of the above theorem is slightly different from the statement in Beck and Khan [1]. The statement in [1] is as follows:

“Let $R \subseteq [0, 1]^2$ be a measurable set having the following property that for every $\epsilon > 0$, there exists a finite collection of non-overlapping rectangles $\{R_1, R_2, \dots, R_k\}$ such that $\cup_{i=1}^k R_i \subseteq R$ and $\mathrm{area}(R \setminus \cup_{i=1}^k R_i) < \epsilon$. Then

$$\lim_{n \rightarrow \infty} \frac{\mathrm{cardinality}(\mathrm{Image}(f_n) \cap R)}{\varphi(n)} = \mathrm{area}(R)”$$

(see Theorem 2 of [1]).

2000 *Mathematics Subject Classification.* 11C20, 11T23.

Key words and phrases. Matrices; Finite fields; Uniform distribution; Character sum.

The original assumption should be strengthened. Otherwise there is a counterexample as follows:

Let $R_1 = [0, 1/2]^2$ and $R_2 = \{(x, y) \in [0, 1]^2 \mid x, y \in \mathbb{Q}\}$. Denote by $R = R_1 \cup R_2$. Since $\text{area}(R_2) = 0$, we have $\text{area}(R) = \text{area}(R_1) = 1/4$. So R satisfies the conditions in the statement of Theorem 2 in [1]. Since the image of f_n are rational points in $[0, 1]^2$ and R contains all the rational points in $[0, 1]^2$, we have $\text{Image}(f_n) \cap R = \text{Image}(f_n)$ for any positive integer n , thus

$$\lim_{n \rightarrow \infty} \frac{\text{cardinality}(\text{Image}(f_n) \cap R)}{\varphi(n)} = 1.$$

But $\text{area}(R) = \text{area}(R_1) = 1/4$, so

$$\lim_{n \rightarrow \infty} \frac{\text{cardinality}(\text{Image}(f_n) \cap R)}{\varphi(n)} \neq \text{area}(R).$$

Notice that, the new conditions in Theorem 1.1 are quite natural. Numerous types of regions satisfy the conditions of Theorem 1.1 such as polygons, disks, annuli lying in the unit square.

Beck and Khan [1, p. 150] remarked that: “In all likelihood this theorem dates back to the late 20’s and early 30’s and was known to mathematicians such as Davenport, Estermann, Kloosterman, Salie.”

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ be the finite field with p elements, $M_n(\mathbb{F}_p)$ be the set of all $n \times n$ matrices over \mathbb{F}_p , $\text{GL}_n(\mathbb{F}_p)$, $\text{SL}_n(\mathbb{F}_p)$ and $\mathcal{Z}_n(\mathbb{F}_p)$ be the group of invertible matrices, the group of matrices of determinant 1 and the set of singular matrices, respectively, where all matrices are from $M_n(\mathbb{F}_p)$.

In this paper, by using Ferguson, Hoffman, Luca, Ostafe and Shparlinski [5]’s recent result for the matrix analogue of classical Kloosterman sums (see Lemma 4.1 below), we show that the above mentioned uniformly distributed phenomenon also exists in $\text{GL}_n(\mathbb{F}_p)$.

For $A = (\overline{a_{ij}}) \in \text{GL}_n(\mathbb{F}_p)$, $A^{-1} = (\overline{b_{ij}})$ denotes the inverse of A .

Let

$$(1.1) \quad g_p : \text{GL}_n(\mathbb{F}_p) \rightarrow \underbrace{[0, 1] \times [0, 1] \cdots \times [0, 1]}_{2n^2}$$

$$A = (\overline{a_{ij}}) \mapsto \begin{pmatrix} \frac{a_{11}}{p}, & \dots, & \frac{a_{1n}}{p}, & \frac{b_{11}}{p}, & \dots, & \frac{b_{1n}}{p} \\ \frac{a_{21}}{p}, & \dots, & \frac{a_{2n}}{p}, & \frac{b_{21}}{p}, & \dots, & \frac{b_{2n}}{p} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{a_{n1}}{p}, & \dots, & \frac{a_{nn}}{p}, & \frac{b_{n1}}{p}, & \dots, & \frac{b_{nn}}{p} \end{pmatrix}$$

In fact, we prove the following theorem.

Theorem 1.3. *Let $R \subset [0, 1]^{2n^2}$ be a measurable set having the following property that for every $\epsilon > 0$, there exist two finite collections of non-overlapping rectangles R_1, \dots, R_k and R^1, \dots, R^l such that $\cup_{i=1}^k R_i \subset R \subset \cup_{j=1}^l R^j$, $\text{area}(R \setminus \cup_{i=1}^k R_i) < \epsilon$ and $\text{area}(\cup_{j=1}^l R^j \setminus R) < \epsilon$. Then*

$$\lim_{p \rightarrow \infty} \frac{\text{cardinality}(\text{Image}(g_p) \cap R)}{\#\text{GL}_n(\mathbb{F}_p)} = \text{area}(R).$$

Remark 1.4. A $\text{GL}_n(\mathbb{F}_p)$ analogy of the uniform distribution on modular hyperbolas can also be established using the same procedure for the proof of the above theorem (see Remark 3.1 below).

Furthermore, let

$$(1.2) \quad h_p : \text{GL}_n(\mathbb{F}_p) \rightarrow \underbrace{[0, 1] \times [0, 1] \cdots \times [0, 1]}_{n^2}$$

$$A = (\overline{a_{ij}}) \mapsto \begin{pmatrix} \frac{a_{11}}{p}, & \cdots, & \frac{a_{1n}}{p} \\ \frac{a_{21}}{p}, & \cdots, & \frac{a_{2n}}{p} \\ \vdots & \vdots & \vdots \\ \frac{a_{n1}}{p}, & \cdots, & \frac{a_{nn}}{p} \end{pmatrix}$$

$$(1.3) \quad s_p : \text{SL}_n(\mathbb{F}_p) \rightarrow \underbrace{[0, 1] \times [0, 1] \cdots \times [0, 1]}_{n^2}$$

$$A = (\overline{a_{ij}}) \mapsto \begin{pmatrix} \frac{a_{11}}{p}, & \cdots, & \frac{a_{1n}}{p} \\ \frac{a_{21}}{p}, & \cdots, & \frac{a_{2n}}{p} \\ \vdots & \vdots & \vdots \\ \frac{a_{n1}}{p}, & \cdots, & \frac{a_{nn}}{p} \end{pmatrix}$$

Using the same methods, and Ferguson, Hoffman, Luca, Ostafe and Shparlinski [5]'s results for the character sum estimations along $\mathcal{Z}_n(\mathbb{F}_p)$ and $\text{SL}_n(\mathbb{F}_p)$ (see Lemmas 2.2, 2.3 and 2.4 below), we can also obtain the following two results.

Theorem 1.5. *Let $R \subseteq [0, 1]^{n^2}$ be a measurable set having the same property as in Theorem 1.3. Then*

$$\lim_{p \rightarrow \infty} \frac{\text{cardinality}(\text{Image}(h_p) \cap R)}{\#\text{GL}_n(\mathbb{F}_p)} = \text{area}(R).$$

Theorem 1.6. *Assumption as above, then*

$$\lim_{p \rightarrow \infty} \frac{\text{cardinality}(\text{Image}(s_p) \cap R)}{\#\text{SL}_n(\mathbb{F}_p)} = \text{area}(R).$$

2. PRELIMINARIES

We need some lemmas to prove the main theorems.

First, we recall some results in [5].

Given two matrices $U = (u_{ij}), X = (x_{ij}) \in M_n(\mathbb{F}_p)$, their product is defined by

$$U \cdot X = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} u_{ij} x_{ij}$$

(see [5, p. 503]).

Let q be a power of a prime number, Ψ be a fixed nonprincipal additive character of \mathbb{F}_q . For $\mathcal{M}, U, V \in M_n(\mathbb{F}_q)$, let

$$K(\mathrm{GL}_n(\mathbb{F}_q), U, V, \mathcal{M}) = \sum_{X \in \mathrm{GL}_n(\mathbb{F}_q)} \Psi(U \cdot X + V \cdot (\mathcal{M}X^{-1}))$$

be the matrix analogue of classical Kloosterman sums (see [5, p. 505]) and

$$\begin{aligned} S(\mathrm{GL}_n(\mathbb{F}_q), U) &= \sum_{X \in \mathrm{GL}_n(\mathbb{F}_q)} \Psi(U \cdot X), \\ S(\mathrm{SL}_n(\mathbb{F}_q), U) &= \sum_{X \in \mathrm{SL}_n(\mathbb{F}_q)} \Psi(U \cdot X), \\ S(\mathcal{Z}_n(\mathbb{F}_q), U) &= \sum_{X \in \mathcal{Z}_n(\mathbb{F}_q)} \Psi(U \cdot X). \end{aligned}$$

The authors in [5] obtained the following results.

Lemma 2.1. (see [5, p. 505]) *Uniformly over all matrices $U, V \in M_n(\mathbb{F}_q)$ among which at least one is a nonzero matrix, and $\mathcal{M} \in \mathrm{GL}_n(\mathbb{F}_q)$, we have*

$$K(\mathrm{GL}_n(\mathbb{F}_q), U, V, \mathcal{M}) \ll q^{n^2-1/2},$$

where the implied constant in the symbol “ \ll ” depends only on n .

Lemma 2.2. (see [5, p. 503]) *Uniformly over all nonzero matrices $U \in M_n(\mathbb{F}_q)$, we have*

$$S(\mathcal{Z}_n(\mathbb{F}_q), U) = O(q^{n^2-5/2}),$$

where the implied constant in the symbol “ O ” depends only on n .

Lemma 2.3. *Uniformly over all nonzero matrices $U \in M_n(\mathbb{F}_q)$, we have*

$$S(\mathrm{GL}_n(\mathbb{F}_q), U) = O(q^{n^2-5/2}),$$

where the implied constant in the symbol “ O ” depends only on n .

Proof. For any nonzero matrix $U \in M_n(\mathbb{F}_q)$, $\bar{\Psi}(X) = \Psi(U \cdot X)$ is also a nontrivial additive character on $M_n(\mathbb{F}_q)$, so we have

$$S(\mathcal{Z}_n(\mathbb{F}_q), U) + S(\mathrm{GL}_n(\mathbb{F}_q), U) = \sum_{X \in M_n(\mathbb{F}_q)} \Psi(U \cdot X) = 0.$$

From Lemma 2.2, we obtain the result. \square

If $\mathbf{u}_1 \cdot \mathbf{x}_1, \dots, \mathbf{u}_n \cdot \mathbf{x}_n$ are all nonzero, then $K(X, U, V)$ is the Hyper-Kloosterman Sum. Delinge proved that it has bound $O(q^{(n-1)/2})$ (see Example 2 in [7]).

Using Delinge’s bound on Hyper-Kloosterman sum (see Example 2 in [7]), we give an alternative proof of the following Lemma of [5].

Lemma 2.4. (see [5, p. 504]) *Uniformly over all nonzero matrices $U \in M_n(\mathbb{F}_q)$, we have*

$$S(\mathrm{SL}_n(\mathbb{F}_q), U) = O(q^{n^2-2}),$$

where the implied constant in the symbol “ O ” depends only on n .

Proof.

$$\begin{aligned}
& S(\mathrm{SL}_n(\mathbb{F}_q), U) \\
&= \frac{1}{(q-1)^{n-1}} \sum_{\lambda_1 \lambda_2 \dots \lambda_n = 1} \sum_{X \in \mathrm{SL}_n(\mathbb{F}_q)} \Psi \left(U \cdot \left(\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} X \right) \right) \\
&= \sum_{X \in \mathrm{SL}_n(\mathbb{F}_q)} \frac{1}{(q-1)^{n-1}} \cdot \sum_{\lambda_1 \lambda_2 \dots \lambda_n = 1} \Psi(\lambda_1 \mathbf{u}_1 \cdot \mathbf{x}_1 + \dots + \lambda_n \mathbf{u}_n \cdot \mathbf{x}_n),
\end{aligned}$$

where \mathbf{u}_i and \mathbf{x}_i are the i -th row of U and X , respectively, with $1 \leq i \leq n$.

Let

$$K(X, U) = \sum_{\lambda_1 \lambda_2 \dots \lambda_n = 1} \Psi(\lambda_1 \mathbf{u}_1 \cdot \mathbf{x}_1 + \dots + \lambda_n \mathbf{u}_n \cdot \mathbf{x}_n).$$

If $\mathbf{u}_1 \cdot \mathbf{x}_1, \dots, \mathbf{u}_n \cdot \mathbf{x}_n$ are all nonzero, then $K(X, U)$ is the Hyper-Kloosterman Sum. Deligne proved that (see Example 2 in [7]),

$$K(X, U) \ll q^{(n-1)/2}.$$

If one of $\mathbf{u}_1 \cdot \mathbf{x}_1, \dots, \mathbf{u}_n \cdot \mathbf{x}_n$ is zero but not all of them are zero, say, $\mathbf{u}_n \cdot \mathbf{x}_n$ is zero, then $K(X, U)$ equals to

$$\sum_{\lambda_1} \Psi(\lambda_1 \mathbf{u}_1 \cdot \mathbf{x}_1) \sum_{\lambda_2} \Psi(\lambda_2 \mathbf{u}_2 \cdot \mathbf{x}_2) \dots \sum_{\lambda_{n-1}} \Psi(\lambda_{n-1} \mathbf{u}_{n-1} \cdot \mathbf{x}_{n-1}).$$

Since at least one factor of the above product is -1 , we have

$$K(X, U) \ll q^{n-2}.$$

If $\mathbf{u}_1 \cdot \mathbf{x}_1, \dots, \mathbf{u}_n \cdot \mathbf{x}_n$ are all zero, we have no cancellation, i.e., $K(X, U) = (q-1)^{n-1}$. But the number of such $X \in \mathrm{SL}_n(\mathbb{F}_q)$ are bound by $O(q^{n-2})$. Moreover, we have $\#\mathrm{SL}_n(\mathbb{F}_p) = p^{n^2-1} + O(p^{n^2-3})$.

Summing all above up, we prove that

$$S(\mathrm{SL}_n(\mathbb{F}_q), U) = O(q^{n^2-2}).$$

□

Remark 2.5. Recently, we obtained explicit expressions of $S(\mathrm{GL}_n(\mathbb{F}_q), U)$ and $S(\mathrm{SL}_n(\mathbb{F}_q), U)$. (See [2] Theorem 2.1 and Theorem 2.2). Such expressions only involve Gauss sums and Kloosterman sums. As a consequence, we got

$$S(\mathrm{GL}_n(\mathbb{F}_q), U) = O(q^{n^2-n}),$$

$$S(\mathrm{SL}_n(\mathbb{F}_q), U) = O(q^{n^2-n}) = O(\max\{q^{n^2-n-1}, q^{(n^2-1)/2}\}).$$

Next we recall Erdős-Turán-Koksma's inequality for the discrepancy of sequences.

Let $B = [a_1, b_1] \times \dots \times [a_k, b_k] \subseteq [0, 1]^k$ be a rectangle, (\mathbf{x}_n) be a sequence in $[0, 1]^k$, and $A(B, N, \mathbf{x}_n)$ be the number of points \mathbf{x}_n , $1 \leq n \leq N$, such that $\mathbf{x}_n \in B$, i.e.

$$A(B, N, \mathbf{x}_n) = \sum_{n=1}^N \chi_B(\mathbf{x}_n),$$

where χ_B is the characteristic function of B .

Definition 2.6. (see [3, p.4] or [8, p.62]) Let $\{\mathbf{x}_1, \dots, \mathbf{x}_N\}$ be a finite sequence of points in $[0, 1]^k$. Then the number

$$D_N = D_N(\mathbf{x}_1, \dots, \mathbf{x}_N) = \sup_{B \subseteq [0,1]^k} \left| \frac{A(B, N, \mathbf{x}_n)}{N} - \text{area}(B) \right|$$

is called the discrepancy of the given sequence, where B runs over all rectangles located in $[0, 1]^k$.

Set $e(x) = \exp(2\pi i x)$ and denote the usual inner product in \mathbb{R}^k by $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^k \mathbf{x}_i \mathbf{y}_i$.

The Erdős-Turán-Koksma inequality provides an upper bound for the discrepancy.

Lemma 2.7. (see [3, p.15] or [8, p.63]) Let $\{\mathbf{x}_1, \dots, \mathbf{x}_N\}$ be a finite sequence of points in $[0, 1]^k$ and H an arbitrary positive integer. Then

$$D_N \leq \left(\frac{3}{2}\right)^k \left(\frac{2}{H+1} + \sum_{0 < \|\mathbf{h}\|_\infty \leq H} \frac{1}{r(\mathbf{h})} \left| \frac{1}{N} \sum_{n=1}^N e(\mathbf{h} \cdot \mathbf{x}_n) \right| \right),$$

where $r(\mathbf{h}) = \prod_{i=1}^k \max\{1, |h_i|\}$ and $\|\mathbf{h}\|_\infty = \max\{|h_i| \mid 1 \leq i \leq k\}$, for $\mathbf{h} = (h_1, \dots, h_k) \in \mathbb{Z}^k$.

3. PROOFS OF MAIN RESULTS

Proof of Theorem 1.3:

We only need to prove the case that $R = [a_1, b_1) \times \dots \times [a_k, b_k) \subset [0, 1]^k$ is a rectangle. The reason is as follows:

Assume the theorem holds for R being a rectangle. Let R be a measurable set as in the assumptions. For every $\epsilon > 0$, let R_1, \dots, R_k and R^1, \dots, R^l be two finite collections of non-overlapping rectangles such that

$$(3.1) \quad \bigcup_{i=1}^k R_i \subseteq R \subseteq \bigcup_{j=1}^l R^j, \quad \text{area}(R \setminus \bigcup_{i=1}^k R_i) < \epsilon \text{ and } \text{area}(\bigcup_{j=1}^l R^j \setminus R) < \epsilon.$$

Then

$$(3.2) \quad \sum_{i=1}^k \text{area}(R_i) \leq \text{area}(R) \leq \sum_{j=1}^l \text{area}(R^j),$$

$$\sum_{i=1}^k \frac{\#(\text{Image}(g_p) \cap R_i)}{\#\text{GL}_n(\mathbb{F}_p)} \leq \frac{\#(\text{Image}(g_p) \cap R)}{\#\text{GL}_n(\mathbb{F}_p)} \leq \sum_{j=1}^l \frac{\#(\text{Image}(g_p) \cap R^j)}{\#\text{GL}_n(\mathbb{F}_p)}.$$

Taking p sufficiently large, the left hand (resp. right hand) sides of the above two inequalities are sufficiently close, i.e, there exists M such that if $p > M$ then

$$(3.3) \quad \left| \sum_{i=1}^k \frac{\#(\text{Image}(g_p) \cap R_i)}{\#\text{GL}_n(\mathbb{F}_p)} - \sum_{i=1}^k \text{area}(R_i) \right| < \epsilon,$$

$$\left| \sum_{j=1}^l \frac{\#(\text{Image}(g_p) \cap R^j)}{\#\text{GL}_n(\mathbb{F}_p)} - \sum_{j=1}^l \text{area}(R^j) \right| < \epsilon.$$

From inequalities (3.1), (3.2) and (3.3), for $p > M$, we have

$$\begin{aligned}
& \frac{\#(\text{Image}(g_p) \cap R)}{\#\text{GL}_n(\mathbb{F}_p)} - \text{area}(R) \\
& \leq \sum_{j=1}^l \frac{\#(\text{Image}(g_p) \cap R^j)}{\#\text{GL}_n(\mathbb{F}_p)} - \text{area}(R) \\
& = \sum_{j=1}^l \frac{\#(\text{Image}(g_p) \cap R^j)}{\#\text{GL}_n(\mathbb{F}_p)} - \sum_{j=1}^l \text{area}(R_j) + \sum_{j=1}^l \text{area}(R_j) - \text{area}(R) \\
& < 2\epsilon.
\end{aligned}$$

Similarly,

$$-2\epsilon < \frac{\#(\text{Image}(g_p) \cap R)}{\#\text{GL}_n(\mathbb{F}_p)} - \text{area}(R).$$

Thus

$$\left| \frac{\#(\text{Image}(g_p) \cap R)}{\#\text{GL}_n(\mathbb{F}_p)} - \text{area}(R) \right| < 2\epsilon.$$

This implies that

$$\lim_{p \rightarrow \infty} \frac{\text{cardinality}(\text{Image}(g_p) \cap R)}{\#\text{GL}_n(\mathbb{F}_p)} = \text{area}(R).$$

Now we prove the fundamental case in which R is the rectangle $[a_1, b_1] \times \cdots \times [a_k, b_k]$.

In Lemma 2.7, viewing the points \mathbf{x} in $\text{Image}(g_p)$ as a sequence in $[0, 1)^k$, where $N = \#\text{GL}_n(\mathbb{F}_p)$ and $k = 2n^2$, we have

$$\begin{aligned}
(3.4) \quad & \left| \frac{\text{cardinality}(\text{Image}(g_p) \cap R)}{\#\text{GL}_n(\mathbb{F}_p)} - \text{area}(R) \right| \\
& \ll \frac{2}{H+1} + \sum_{0 < \|\mathbf{h}\|_\infty \leq H} \frac{1}{r(\mathbf{h})} \left| \frac{1}{\#\text{GL}_n(\mathbb{F}_p)} \sum_{\mathbf{x} \in \text{Image}(g_p)} e(\mathbf{h} \cdot \mathbf{x}) \right|,
\end{aligned}$$

where $r(\mathbf{h}) = \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \max\{1, |h_{ij}|\}$ for

$$\mathbf{h} = \begin{pmatrix} h_{11}, & \dots, & h_{1n}, & h_{(n+1)1}, & \dots, & h_{(n+1)n} \\ h_{21}, & \dots, & h_{2n}, & h_{(n+2)1}, & \dots, & h_{(n+2)n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{n1}, & \dots, & h_{nn}, & h_{(2n)1}, & \dots, & h_{(2n)n} \end{pmatrix}$$

in \mathbb{Z}^{2n^2} .

From the definition of g_p , we have

$$\begin{aligned}
(3.5) \quad e(\mathbf{h} \cdot \mathbf{x}) &= e\left(\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \frac{a_{ij}}{p} \cdot h_{ij} + \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \frac{b_{ij}}{p} \cdot h_{(n+i)j} \right) \\
&= e_p\left(\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} a_{ij} \cdot h_{ij} + \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} b_{ij} \cdot h_{(n+i)j} \right),
\end{aligned}$$

where $e_p(z) = \exp(2\pi iz/p)$.

If $(h_{ij}, p) = p$, for any i, j , then $r(\mathbf{h}) = \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \max\{1, |h_{ij}|\} \geq p$, thus

$$(3.6) \quad \frac{1}{r(\mathbf{h})} \left| \frac{1}{\#\mathrm{GL}_n(\mathbb{F}_p)} \sum_{\mathbf{x} \in \mathrm{Image}(g_p)} e(\mathbf{h} \cdot \mathbf{x}) \right| \leq \frac{1}{p} < \frac{1}{p^{1/2}}.$$

If $(h_{ij}, p) = 1$, for some i, j , in Lemma 4.1, take $\mathcal{M} = I, U = (\overline{h_{ij}})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}, V = (\overline{h_{(n+i)j}})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}, X = A$, and at least one of U, V is a nonzero matrix, we have

$$(3.7) \quad \begin{aligned} \sum_{\mathbf{x} \in \mathrm{Image}(g_p)} e(\mathbf{h} \cdot \mathbf{x}) &= \sum_{A = (\overline{a_{ij}}) \in \mathrm{GL}_n(\mathbb{F}_p)} e_p \left(\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} a_{ij} \cdot h_{ij} + \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} b_{ij} \cdot h_{(n+i)j} \right) \\ &= K(\mathrm{GL}_n(\mathbb{F}_p), U, V, \mathcal{M}) \\ &\ll p^{n^2-1/2}, \end{aligned}$$

since $\#\mathrm{GL}_n(\mathbb{F}_p) = p^{n^2} + O(p^{n^2-1})$, from (3.7), we have

$$(3.8) \quad \frac{1}{r(\mathbf{h})} \left| \frac{1}{\#\mathrm{GL}_n(\mathbb{F}_p)} \sum_{\mathbf{x} \in \mathrm{Image}(g_p)} e(\mathbf{h} \cdot \mathbf{x}) \right| \ll \frac{1}{p^{1/2}}.$$

Notice that

$$(3.9) \quad \#\{\mathbf{h} \in \mathbb{Z}^{2n^2} | 0 < \|\mathbf{h}\|_\infty \leq H\} \ll H^{2n^2}.$$

From (3.4), (3.6), (3.8), (3.9), and taking $H = \lfloor p^{1/(2(2n^2+1))} \rfloor$, we get

$$(3.10) \quad \begin{aligned} &\left| \frac{\text{cardinality}(\mathrm{Image}(g_p) \cap R)}{\#\mathrm{GL}_n(\mathbb{F}_p)} - \text{area}(R) \right| \\ &\ll \frac{2}{H+1} + H^{2n^2} \frac{1}{p^{1/2}} \\ &\ll \frac{1}{p^{1/(2(2n^2+1))}}. \end{aligned}$$

Letting $\lim_{p \rightarrow \infty}$ in (3.10), we get our result.

Remark 3.1. For any fixed $C = (\overline{a_{ij}}) \in \mathrm{GL}_n(\mathbb{F}_p)$, we consider the matrix equation $BA = C$, where $A = (\overline{a_{ij}})$, $B = (\overline{b_{ij}})$ in $\mathrm{GL}_n(\mathbb{F}_p)$.

Let

$$(3.11) \quad \tilde{g}_p : \mathrm{GL}_n(\mathbb{F}_p) \rightarrow \underbrace{[0, 1] \times [0, 1] \cdots \times [0, 1]}_{2n^2}$$

$$A = (\overline{a_{ij}}) \mapsto \begin{pmatrix} \frac{a_{11}}{p}, & \cdots, & \frac{a_{1n}}{p}, & \frac{b_{11}}{p}, & \cdots, & \frac{b_{1n}}{p} \\ \frac{a_{21}}{p}, & \cdots, & \frac{a_{2n}}{p}, & \frac{b_{21}}{p}, & \cdots, & \frac{b_{2n}}{p} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{a_{n1}}{p}, & \cdots, & \frac{a_{nn}}{p}, & \frac{b_{n1}}{p}, & \cdots, & \frac{b_{nn}}{p} \end{pmatrix}.$$

The same procedure can show Theorem 1.3 is also established for \tilde{g}_p . The only change is that we take $\mathcal{M} = C, U = (h_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}, V = (h_{(n+i)j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ and

$X = A$ in Lemma 4.1. This can be viewed as a $\mathrm{GL}_n(\mathbb{F}_p)$ analogy of the uniform distribution on modular hyperbolas.

Proof of Theorem 1.5:

The method is exactly the same as in Theorem 1.3, except that we replace the estimation of $K(\mathrm{GL}_n(\mathbb{F}_p), U, V, \mathcal{M})$ by the estimation of $S(\mathrm{GL}_n(\mathbb{F}_p), U)$ (see Lemma 2.3).

Proof of Theorem 1.6:

The method is exactly the same as in Theorem 1.3, except that we replace the estimation of $K(\mathrm{GL}_n(\mathbb{F}_p), U, V, \mathcal{M})$ by the estimation of $S(\mathrm{SL}_n(\mathbb{F}_p), U)$ (see Lemma 2.4) and notice that $\#\mathrm{SL}_n(\mathbb{F}_p) = p^{n^2-1} + O(p^{n^2-3})$.

4. QUESTIONS ON SPECIAL LINEAR GROUPS

In this section, we discuss the following questions:

Is the image of $\mathrm{SL}_n(\mathbb{F}_p)$ under g_p (see (1.1)), uniformly distributed in $[0, 1]^{2n^2}$?

In the sequel, we will show that for $n \leq 2$, the answer is negative. For $n \geq 3$, we prove it is true.

The case $n = 1$ is trivial.

For $n = 2$, since

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}^{-1} = \begin{pmatrix} \bar{d} & -\bar{b} \\ -\bar{c} & \bar{a} \end{pmatrix}, \text{ where } \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p),$$

one can easily find a nonzero vector

$$\mathbf{h} = \begin{pmatrix} h_{11} & h_{12} & h_{13} & h_{14} \\ h_{21} & h_{22} & h_{23} & h_{24} \end{pmatrix} \in \mathbb{Z}^8$$

such that

$$\mathbf{x} \mapsto e(\mathbf{h} \cdot \mathbf{x}) = 1, \text{ for all } \mathbf{x} \in g_p(\mathrm{SL}_2(\mathbb{F}_p)).$$

For example, take arbitrary nonzero \mathbf{h} with $h_{11} + h_{24} = 0$, $h_{12} - h_{14} = 0$, $h_{13} + h_{22} = 0$ and $h_{21} - h_{23} = 0$.

Hence

$$\lim_{p \rightarrow \infty} \frac{1}{\#\mathrm{SL}_2(\mathbb{F}_p)} \sum_{\mathbf{x} \in g_p(\mathrm{SL}_2(\mathbb{F}_p))} e(\mathbf{h} \cdot \mathbf{x}) \neq \int_{[0,1]^8} e(\mathbf{h} \cdot \mathbf{x}) d\mathbf{x}.$$

This implies that the image of $\mathrm{SL}_2(\mathbb{F}_p)$ under g_p is not uniformly distributed, that is, Theorem 1.3 does not hold for $\mathrm{SL}_2(\mathbb{F}_p)$.

For the case $n \geq 3$, the element and its inverse of $\mathrm{SL}_n(\mathbb{F}_p)$ is uniformly distributed. The reason is as follows.

The uniform distributed property of $\mathrm{SL}_n(\mathbb{F}_q)$ relies on the estimation of the following exponential sum

$$K(\mathrm{SL}_n(\mathbb{F}_q), U, V) = \sum_{X \in \mathrm{SL}_n(\mathbb{F}_q)} \Psi(U \cdot X + V \cdot X^{-1})$$

where $U, V \in M_n(\mathbb{F}_q)$, at least one of which is nonzero.

Lemma 4.1. *Let $n \geq 3$. Uniformly over all matrices $U, V \in M_n(\mathbb{F}_q)$ among which at least one is a nonzero matrix, we have*

$$K(\mathrm{SL}_n(\mathbb{F}_q), U, V) \ll q^{n^2-2},$$

where the implied constant in the symbol “ \ll ” depends only on n .

Proof. First assume $n = 2m$ is even, where $m \geq 2$. Since at least one of U, V is nonzero, without loss generality, we can assume the first row of U is not zero. Let $B \in M_m(\mathbb{F}_q)$ be a $m \times m$ square matrix. We have

$$\begin{pmatrix} I_m & B \\ 0 & I_m \end{pmatrix}^{-1} = \begin{pmatrix} I_m & -B \\ 0 & I_m \end{pmatrix}.$$

Then

$$\begin{aligned} (4.1) \quad & K(\mathrm{SL}_n(\mathbb{F}_q), U, V) \\ &= \frac{1}{q^{m^2}} \sum_{B \in M_m(\mathbb{F}_q)} \sum_{X \in \mathrm{SL}_n(\mathbb{F}_q)} \Psi \left(U \cdot \left(\begin{pmatrix} I_m & B \\ 0 & I_m \end{pmatrix} X \right) + V \cdot \left(X^{-1} \begin{pmatrix} I_m & -B \\ 0 & I_m \end{pmatrix} \right) \right) \\ &= \sum_{X \in \mathrm{SL}_n(\mathbb{F}_q)} \Psi(U \cdot X + V \cdot X^{-1}) \\ &\quad \cdot \frac{1}{q^{m^2}} \sum_{B \in M_m(\mathbb{F}_q)} \Psi \left(U \cdot \left(\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} X \right) + V \cdot \left(X^{-1} \begin{pmatrix} 0 & -B \\ 0 & 0 \end{pmatrix} \right) \right). \end{aligned}$$

For $1 \leq i \leq n$, let \mathbf{u}_i be the i -th row of U , $\tilde{\mathbf{v}}_i$ the i -th column of V , \mathbf{x}_i the i -th row of X , and $\widetilde{\mathbf{x}_i^{-1}}$ the i -th column of X^{-1} . Below, we will use the notation $\mathbf{u}_i \cdot \mathbf{x}_i$ and $\tilde{\mathbf{v}}_i \cdot \widetilde{\mathbf{x}_i^{-1}}$ to represent the standard inner vector product.

We have

$$\begin{aligned} (4.2) \quad & \sum_{B \in M_m(\mathbb{F}_q)} \Psi \left(U \cdot \left(\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} X \right) + V \cdot \left(X^{-1} \begin{pmatrix} 0 & -B \\ 0 & 0 \end{pmatrix} \right) \right) \\ &= \sum_{(b_{ij}) \in M_m(\mathbb{F}_q)} \Psi \left(\mathbf{u}_1 \cdot \sum_{j=m+1}^{2m} b_{1j} \mathbf{x}_j + \dots + \mathbf{u}_m \cdot \sum_{j=m+1}^{2m} b_{mj} \mathbf{x}_j \right. \\ &\quad \left. - \widetilde{\mathbf{v}}_{m+1} \cdot \sum_{i=1}^m \widetilde{\mathbf{x}_i^{-1}} b_{i \ m+1} - \dots - \widetilde{\mathbf{v}}_{2m} \cdot \sum_{i=1}^m \widetilde{\mathbf{x}_i^{-1}} b_{i \ 2m} \right) \\ &= \sum_{(b_{ij}) \in M_m(\mathbb{F}_q)} \Psi \left(\sum_{i=1}^m \sum_{j=m+1}^{2m} (\mathbf{u}_i \cdot \mathbf{x}_j - \tilde{\mathbf{v}}_j \cdot \widetilde{\mathbf{x}_i^{-1}}) \times b_{ij} \right) \\ &= \prod_{i=1}^m \prod_{j=m+1}^{2m} \sum_{b_{ij} \in \mathbb{F}_q} \Psi \left((\mathbf{u}_i \cdot \mathbf{x}_j - \tilde{\mathbf{v}}_j \cdot \widetilde{\mathbf{x}_i^{-1}}) \times b_{ij} \right) \\ &= \prod_{i=1}^m \prod_{j=m+1}^{2m} \sum_{b_{ij} \in \mathbb{F}_q} \Psi \left((\mathbf{u}_i \cdot \mathbf{x}_j - \det(\mathbf{x}_1^t, \dots, \mathbf{x}_{i-1}^t, \tilde{\mathbf{v}}_j, \mathbf{x}_{i+1}^t, \dots, \mathbf{x}_n^t) \times b_{ij} \right), \end{aligned}$$

where \mathbf{x}_i^t is the transpose of \mathbf{x}_i with $1 \leq i \leq n$. The last equality is because: from $XX^{-1} = I$, we get $\mathbf{x}_j^t \cdot \widetilde{\mathbf{x}_i^{-1}} = \mathbf{x}_j \mathbf{x}_i^{-1} = \delta_{ji}$. Therefore, the linear function

$$\widetilde{\mathbf{y}} \longmapsto \widetilde{\mathbf{y}} \cdot \widetilde{\mathbf{x}_i^{-1}}$$

must agree with the linear function

$$\widetilde{\mathbf{y}} \longmapsto \det(\mathbf{x}_1^t, \dots, \mathbf{x}_{i-1}^t, \widetilde{\mathbf{y}}, \mathbf{x}_{i+1}^t, \dots, \mathbf{x}_n^t).$$

Let N be the number of matrices $X \in \mathrm{SL}_n(\mathbb{F}_q)$ whose rows satisfy the equations:

$$(4.3) \quad \mathbf{u}_i \cdot \mathbf{x}_j - \det(\mathbf{x}_1^t, \dots, \mathbf{x}_{i-1}^t, \widetilde{\mathbf{v}}_j, \mathbf{x}_{i+1}^t, \dots, \mathbf{x}_n^t) = 0,$$

where $1 \leq i \leq m$, $m+1 \leq j \leq 2m$.

Combining equations (4.1), (4.2), and from the orthogonality of characters, we get

$$(4.4) \quad |K(\mathrm{SL}_n(\mathbb{F}_q), U, V)| \leq N.$$

Note that we already assumed $\mathbf{u}_1 \neq 0$. Take $i = 1$ $j = m+1$ in (4.3). We get

$$(4.5) \quad \mathbf{u}_1 \cdot \mathbf{x}_{m+1} - \det(\widetilde{\mathbf{v}_{m+1}}, \mathbf{x}_2^t, \dots, \mathbf{x}_{m+1}^t, \dots, \mathbf{x}_n^t) = 0.$$

Fixed $\mathbf{x}_2, \dots, \mathbf{x}_m, \mathbf{x}_{m+2}, \dots, \mathbf{x}_n$, viewing (4.5) as a linear function of \mathbf{x}_{m+1} , if it is nontrivial, then the choices of \mathbf{x}_{m+1} satisfying (4.5) is q^{n-1} . Otherwise, (4.5) is always zero. Substituting \mathbf{x}_{m+1} for \mathbf{x}_i with $2 \leq i \leq n$, $i \neq m+1$, we get $\mathbf{u}_1 \cdot \mathbf{x}_i = 0$. So the number of $\mathbf{x}_2, \dots, \mathbf{x}_m, \mathbf{x}_{m+2}, \dots, \mathbf{x}_n$ making (4.5) trivial is at most $q^{(n-1)(n-2)}$. Therefore, the choices of $\mathbf{x}_2, \dots, \mathbf{x}_n$ satisfying (4.5) is

$$O(\max\{q^{n(n-1)-1}, q^{n(n-1)-(n-2)}\}) = O(q^{n(n-1)-1}),$$

since $n \geq 3$. For fixed values of $\mathbf{x}_2, \dots, \mathbf{x}_n$, the number of \mathbf{x}_1 making $\det X = 1$ is $O(q^{n-1})$. Therefore, the number of $X \in \mathrm{SL}_n(\mathbb{F}_q)$ satisfying (4.5) is $O(q^{n^2-2})$. Thus, $N \ll q^{n^2-2}$.

By (4.4), we get the desired result:

$$K(\mathrm{SL}_n(\mathbb{F}_q), U, V) \ll q^{n^2-2},$$

in the case that n is even.

The case n being odd can be handled similarly. We briefly illustrate it. In that case, let $n = 2m - 1$ with $m \geq 2$. Replace the matrix

$$\begin{pmatrix} I_m & B \\ 0 & I_m \end{pmatrix}.$$

in (4.1) by the matrix

$$\begin{pmatrix} I_{m-1} & \widetilde{B} \\ 0 & I_m \end{pmatrix},$$

where \widetilde{B} is a $m-1 \times m$ matrix over \mathbb{F}_q . The rest are the same. \square

Remark 4.2. For $n \geq 3$, the above method can also be applied to $\mathrm{GL}_n(\mathbb{F}_q)$ case, which shows that

$$K(\mathrm{GL}_n(\mathbb{F}_p), U, V, \mathcal{M}) \ll q^{n^2-1},$$

slightly improving the earlier bound $q^{n^2-1/2}$ of [5] (See Lemma 4.1).

REFERENCES

- [1] J. Beck, M. R. Khan, On the uniform distribution of inverse modulo n , Period. Math. Hungar., 44 (2002), 147–155.
- [2] Y. Li, S. Hu, Gauss sums over some matrix groups, arXiv:1105.4513.
- [3] M. Damota, R. F. Tichy, Sequences, Discrepancies and Applications, Lect. Notes in Math., vol. 1652, Springer–Verlag, 1997.
- [4] K. Ford, M. R. Khan, I. E. Shparlinski, C. L. Yankov, On the maximal difference between an element and its inverse in residue rings, Proc. Amer. Math. Soc., 133 (2005), 3463–3468.
- [5] R. Ferguson, C. Hoffman, F. Luca, A. Ostafe, I. E. Shparlinski, Some additive combinatorics problems in matrix rings (arXiv:0902.3482), Rev. Mat. Complut., 23 (2010), 501–513.
- [6] M. R. Khan, I. E. Shparlinski, On the maximal difference between an element and its inverse modulo n , Period. Math. Hungar., 47 (2003), 111–117.
- [7] E. Kowalski, Some aspects and applications of the Riemann hypothesis over finite fields, Milan J. of Mathematics, 78 (2010), 179–220.
- [8] H. Niederreiter, A. Winterhof, Exponential sums for nonlinear recurring sequences, Finite Fields Appl., 14 (2008), 59–64.
- [9] I. E. Shparlinski, A. Winterhof, On the number of distance between the coordinates of points on modular hyperbolas, J. Number Theory, 128 (2008), 1224–1230.
- [10] I. E. Shparlinski, Modular Hyperbolas, arXiv:1103.2879.
- [11] M.-T. Tsai, A. Zaharescu, On the action of permutations on distances between values of rational functions modulo p , Finite fields Appl., in press.
- [12] Wengpeng Zhang, On the distribution of inverse modulo n , J. Number Theory, 61 (1996), 301–310.
- [13] Wengpeng Zhang, On the distribution of primitive roots modulo p , Publ. Math. Debrecen, 53 (1998), 245–255.

DEPARTMENT OF MATHEMATICS, KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY (KAIST), 373-1 GUSEONG-DONG, YUSEONG-GU, DAEJEON 305-701, SOUTH KOREA

E-mail address: hus04@mails.tsinghua.edu.cn, husu@kaist.ac.kr

DEPARTMENT OF APPLIED MATHEMATICS, CHINA AGRICULTURE UNIVERSITY, BEIJING 100083, CHINA

E-mail address: liyan_00@mails.tsinghua.edu.cn